CHAPTER

3

DYNAMIC HOST CONFIGURATION PROTOCOL

After reading this chapter and completing the exercises, you will be able to:

- Describe the dynamic host configuration protocol (DHCP)
- Describe the dynamic IP leasing process
- Configure a client to use DHCP
- Install the DHCP server service
- Configure scopes within the DHCP server service
- Define and create scope options
- Authorize a DHCP server in Active Directory
- Configure DHCP for integration with DNS
- Manage, monitor, and troubleshoot DHCP

Chapter 2 introduced the concept of dynamic IP address assignment. The hands-on exercises showed how to configure a client to obtain an IP address from a Dynamic Host Configuration Protocol (DHCP) server. The entire section on dynamic IP addressing referred to DHCP as the network service responsible for dynamically assigning IP addresses. Unfortunately, the DHCP server does not magically appear on your network. You must install, configure, manage, and monitor it to ensure that clients can obtain dynamic IP addresses.

This chapter explains the process used by clients to obtain dynamic IP addresses from a DHCP server. It also describes how to properly install and configure a Windows 2000 server as a DHCP server. In addition, it tells how to integrate a Windows 2000 DHCP server with WINS and DNS. Finally, you learn some basic monitoring, troubleshooting, and management procedures for Windows 2000 DHCP servers.

Overview of Dynamic Host Configuration Protocol

Network administrators constantly try to ease their overloaded workday. As a result, any network service that reduces manual administration of network clients is a welcome addition to most administrators' toolboxes. DHCP allows client machines that are configured to obtain IP addresses automatically to lease an IP address (and a subnet mask) for a configured amount of time. Clients can also receive much more than just an IP address and subnet mask. With a DHCP server, you can assign options that include everything from the default gateway address to a DNS and a WINS server address. The automatic assignment of IP addresses also reduces the work associated with moving clients between subnets or even between complete networks. For instance, workers who travel constantly from site to site within a company can connect to any network jack, receive correct IP addressing, and begin working, if they have laptops configured to obtain IP addresses via DHCP.

The DHCP server with Windows 2000 supports several important new features:

- *Rogue DHCP server detection*: DHCP servers in an environment with Active Directory fully implemented are required to register their IP address with the DHCP Active Directory object. If an unregistered Windows 2000 DHCP server comes online, its DHCP server service shuts down, and it cannot respond to client DHCPDiscover packets. This prevents unauthorized DHCP servers from providing incorrect information to network clients.
- *Integration with DNS*: The DHCP service in Windows 2000 can use the dynamic DNS protocol to dynamically register **A records** or host records and **pointer (PTR) resource records** for clients that do not support **Dynamic DNS (DDNS)**. This configuration actually requires setting parameters on your DNS servers. The section, "Integrating DHCP and DNS," discusses DNS Intergration in detail.
- *Support for **superscopes***: The Windows 2000 DHCP server supports superscopes, which group several IP address scopes into a single administrative unit. The section, "**Configuring Scopes**," provides more information on superscopes.
- *Support for **multicast scopes***: You can now give multicast addressing information to clients. This feature allows clients to participate in multicast groups.
- *Increased monitoring and management tools*: The DHCP server in Windows 2000 provides new performance counters for System Monitor. These counters allow you to monitor nearly every aspect of DHCP server performance. Windows 2000 also includes the DHCP snap-in for easy management of IP addresses within the **Microsoft Management Console (MMC)** framework.

DHCP Lease Process

A successful DHCP lease process consists of four steps between a client and a server: discover, offer, request, and acknowledgment. Figure 3-1 illustrates the four steps, showing whether the client or server initiates each step.

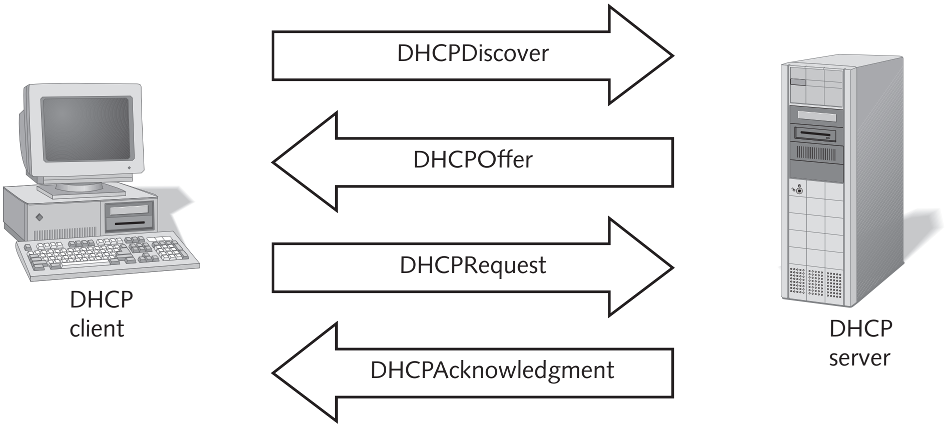


Figure 3-1 Four steps in successful DHCP lease

As shown in Figure 3-1, the client is responsible for starting the process of IP address leasing. Clients broadcast a **DHCPDiscover** packet when they are first turned on or when their current dynamic lease expires and they must obtain a new IP address. In essence, you can think of leasing an IP address as borrowing an address for a set amount of time, the lease duration.

All DHCP servers on the same **network segment** as the client return a **DHCPOffer** that includes a possible IP address that the client may use. The client accepts the first returned offer by requesting it from the DHCP server with a **DHCPRequest** packet. Finally, the DHCP server marks the address as "leased" in its database of addresses (commonly known as scopes) and verifies that the client can use the address with a **DHCPAcknowledgment** (DHCPAck). **Scopes** are continuous ranges of IP addresses that a DHCP server can give to clients. The scopes configured on a server contain the addresses leased to clients.

If for some reason the DHCP server does not verify the address of a client, it issues a **DCHPNack** or negative acknowledgment. This can occur when a client with a dynamic IP address moves to a different network and tries to obtain its previous IP address. Since the old address is not valid for the new network, the DHCP server issues a DHCPNack to force the client to restart the leasing process.

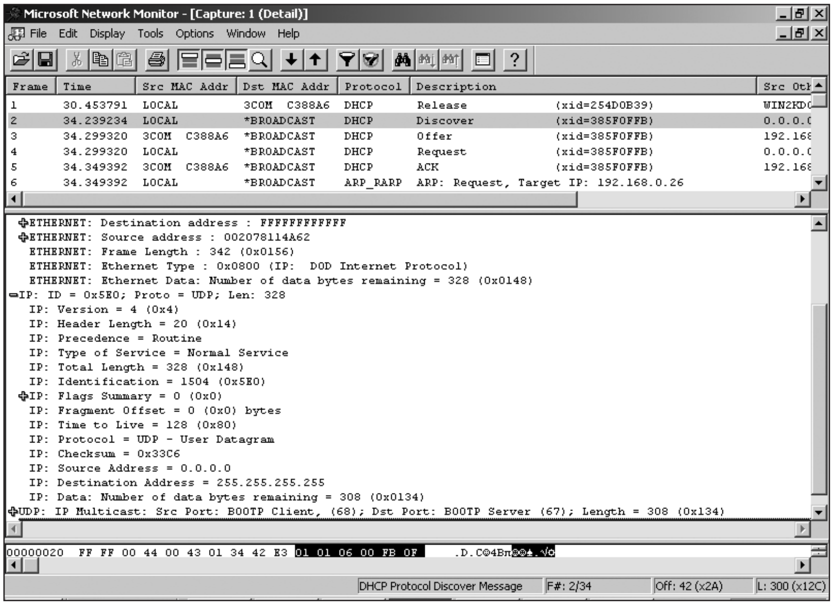
Note

You can easily remember the four steps in the DHCP leasing process using a simple sentence: Aunt **DORA** helps with DHCP addressing. In other words, Aunt **D**iscover, **O**ffer, **R**equest, **A**cknowledgment helps with DHCP addressing.

To understand the DHCP process fully, you need a detailed understanding of exactly what happens in each of the four phases. In the next four sections, you learn exactly what happens.

Step 1: DHCPDiscover

The DHCP client initiates the first step in the DHCP process. When a client is first turned on, its lease expires or it receives a DHCPNack from a DHCP server, it must find a DHCP server on its local segment. All four steps in the DHCP leasing process are broadcast based. In other words, the process sends the DHCP packets to the broadcast MAC address of FFFFFFFFFFFF and the broadcast IP address of 255.255.255.255. Therefore, a DHCP server must be located on the same **broadcast domain** as the client, or the client cannot lease an IP address. Figure 3-2 shows a Network Monitor capture of the DHCP Discover process.


Microsoft Network Monitor - [Capture: 1 (Detail)]
File Edit Display Tools Options Window Help
?

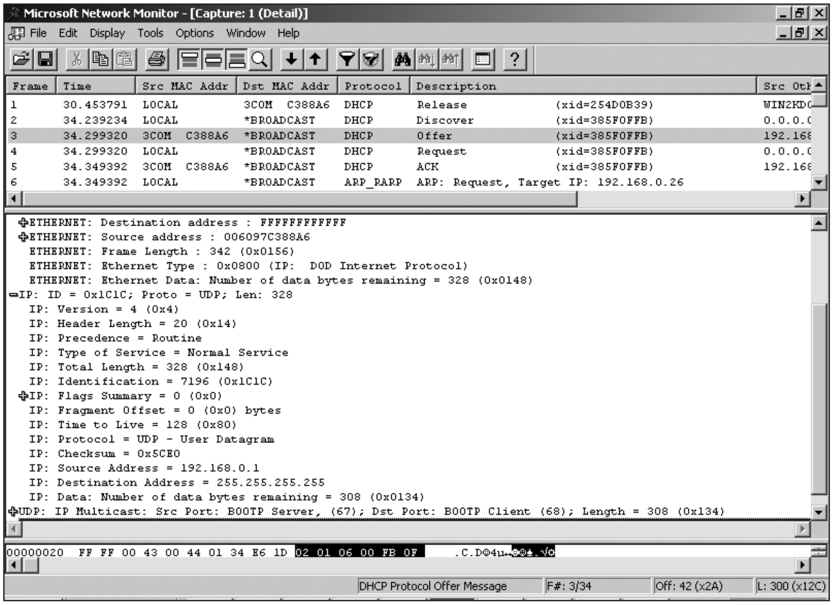
```
Frame   Time       Src MAC Addr   Dst MAC Addr  Protocol  Description                          Src Oth
1       30.453791  LOCAL          3COM  C388A6  DHCP      Release          (xid=254D0B39)      WIN2KDC
2       34.239234  LOCAL          *BROADCAST    DHCP      Discover         (xid=385F0FFB)      0.0.0.0
3       34.299320  3COM  C388A6   *BROADCAST    DHCP      Offer            (xid=385F0FFB)      192.168
4       34.299320  LOCAL          *BROADCAST    DHCP      Request          (xid=385F0FFB)      0.0.0.0
5       34.349392  3COM  C388A6   *BROADCAST    DHCP      ACK              (xid=385F0FFB)      192.168
6       34.349392  LOCAL          *BROADCAST    ARP_RARP  ARP: Request, Target IP: 192.168.0.26

 +ETHERNET: Destination address : FFFFFFFFFFFF
 +ETHERNET: Source address : 002078114A62
  ETHERNET: Frame Length : 342 (0x0156)
  ETHERNET: Ethernet Type : 0x0800 (IP:  DOD Internet Protocol)
  ETHERNET: Ethernet Data: Number of data bytes remaining = 328 (0x0148)
-IP: ID = 0x5E0; Proto = UDP; Len: 328
  IP: Version = 4 (0x4)
  IP: Header Length = 20 (0x14)
  IP: Precedence = Routine
  IP: Type of Service = Normal Service
  IP: Total Length = 328 (0x148)
  IP: Identification = 1504 (0x5E0)
 +IP: Flags Summary = 0 (0x0)
  IP: Fragment Offset = 0 (0x0) bytes
  IP: Time to Live = 128 (0x80)
  IP: Protocol = UDP - User Datagram
  IP: Checksum = 0x33C6
  IP: Source Address = 0.0.0.0
  IP: Destination Address = 255.255.255.255
  IP: Data: Number of data bytes remaining = 308 (0x0134)
+UDP: IP Multicast: Src Port: BOOTP Client, (68); Dst Port: BOOTP Server (67); Length = 308 (0x134)

00000020  FF FF 00 44 00 43 01 34 42 E3 01 01 06 00 FB 0F     .D.C©4Bπ©©±.√☼

DHCP Protocol Discover Message   F#: 2/34   Off: 42 (x2A)   L: 300 (x12C)
```

Figure 3-2 DHCPDiscover packet capture in Network Monitor

As shown in Figure 3-2, the ETHERNET: Destination Address of the DHCPDiscover packet is the broadcast **MAC address** of FFFFFFFFFFFF. The ETHERNET: Source Address is the MAC address of the client initiating the DHCPDiscover packet. The IP: Source Address for the packet is 0.0.0.0 because the client does not have an IP address configured yet. The IP: Destination Address is the broadcast address 255.255.255.255. In short, the DHCPDiscover packet is a broadcast packet at both the MAC layer (layer 2 of the OSI model) and the IP addressing layer (layer 3 of the OSI model). All clients on the local segment can see and examine the DHCPDiscover packet. However, only DHCP servers respond with a DHCPOffer packet.

Step 2: DHCPOffer

All DHCP servers that see the DHCPDiscover packet respond to the client with a DHCPOffer packet. Figure 3-3 shows a DHCPOffer packet.



```
Frame  Time       Src MAC Addr  Dst MAC Addr  Protocol  Description                              Src Oth
1      30.453791  LOCAL         3COM  C388A6  DHCP      Release            (xid=254D0B39)        WIN2KDC
2      34.239234  LOCAL         *BROADCAST    DHCP      Discover           (xid=385F0FFB)        0.0.0.C
3      34.299320  3COM  C388A6  *BROADCAST    DHCP      Offer              (xid=385F0FFB)        192.168
4      34.299320  LOCAL         *BROADCAST    DHCP      Request            (xid=385F0FFB)        0.0.0.C
5      34.349392  3COM  C388A6  *BROADCAST    DHCP      ACK                (xid=385F0FFB)        192.168
6      34.349392  LOCAL         *BROADCAST    ARP_RARP  ARP: Request, Target IP: 192.168.0.26
```

```
 +ETHERNET: Destination address : FFFFFFFFFFFF
 +ETHERNET: Source address : 006097C388A6
  ETHERNET: Frame Length : 342 (0x0156)
  ETHERNET: Ethernet Type : 0x0800 (IP:  DOD Internet Protocol)
  ETHERNET: Ethernet Data: Number of data bytes remaining = 328 (0x0148)
-IP: ID = 0x1C1C; Proto = UDP; Len: 328
  IP: Version = 4 (0x4)
  IP: Header Length = 20 (0x14)
  IP: Precedence = Routine
  IP: Type of Service = Normal Service
  IP: Total Length = 328 (0x148)
  IP: Identification = 7196 (0x1C1C)
 +IP: Flags Summary = 0 (0x0)
  IP: Fragment Offset = 0 (0x0) bytes
  IP: Time to Live = 128 (0x80)
  IP: Protocol = UDP - User Datagram
  IP: Checksum = 0x5CE0
  IP: Source Address = 192.168.0.1
  IP: Destination Address = 255.255.255.255
  IP: Data: Number of data bytes remaining = 308 (0x0134)
+UDP: IP Multicast: Src Port: BOOTP Server, (67); Dst Port: BOOTP Client (68); Length = 308 (0x134)
```

```
00000020  FF FF 00 43 00 44 01 34 E6 1D 02 01 06 00 FB 0F      .C.D©4µ..©©♠.√◊
```

```
DHCP Protocol Offer Message   F#: 3/34   Off: 42 (x2A)   L: 300 (x12C)
```

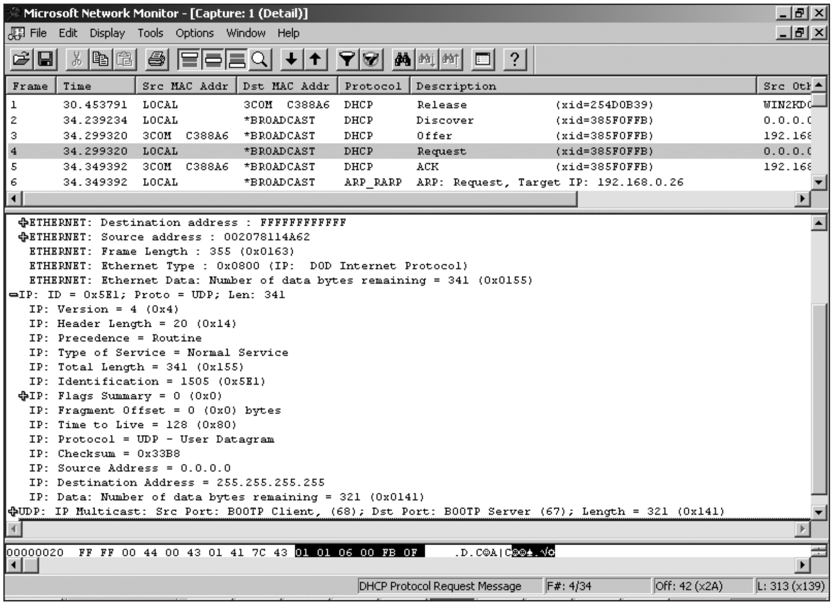
Figure 3-3 DHCPOffer packet capture in Network Monitor

The DHCPOffer packet has an ETHERNET: Destination address of FFFFFFFFFFFF, the broadcast MAC address. The ETHERNET: Source Address is the MAC address of the DHCP server. The IP: Source Address field displays the IP address of the DHCP server. The DHCP server uses this and upper layer information to determine if a client is requesting an IP address from that particular server. The IP: Destination Address is still the broadcast address of 255.255.255.255. The broadcast IP address must be used as the destination because at this point the DHCP client has no IP address.

The client accepts the first DHCPOffer packet it receives from a valid DHCP server and responds with a DHCPRequest packet to obtain the IP address from the DHCP Server.

Step 3: DHCPRequest

The DHCPRequest packet, like every packet in the DHCP process, has an ETHERNET: Destination Address of FFFFFFFFFFFF. The ETHERNET: Source Address is the MAC address of the DHCP client. The IP: Source Address is 0.0.0.0 because the client, although halfway through the lease process, still has no IP address. The IP: Destination Address must remain 255.255.255.255 for this very same reason. Figure 3-4 shows the information discussed about the DHCPRequest packet.

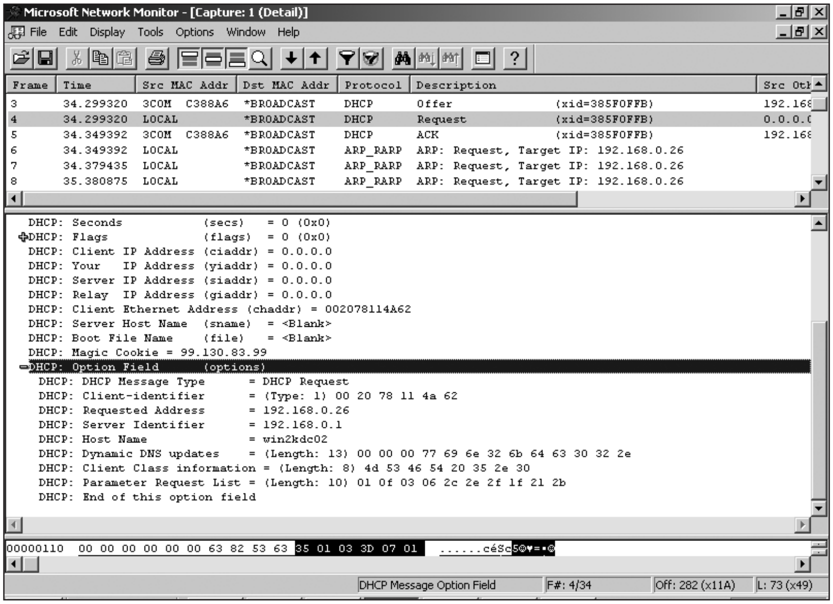


Microsoft Network Monitor - [Capture: 1 (Detail)]
File Edit Display Tools Options Window Help

```
Frame  Time       Src MAC Addr  Dst MAC Addr  Protocol  Description                          Src Oth
1      30.453791  LOCAL         3COM  C388A6  DHCP      Release            (xid=254D0B39)    WIN2KDC
2      34.239234  LOCAL         *BROADCAST    DHCP      Discover           (xid=385F0FFB)    0.0.0.C
3      34.299320  3COM  C388A6  *BROADCAST    DHCP      Offer              (xid=385F0FFB)    192.168
4      34.299320  LOCAL         *BROADCAST    DHCP      Request            (xid=385F0FFB)    0.0.0.C
5      34.349392  3COM  C388A6  *BROADCAST    DHCP      ACK                (xid=385F0FFB)    192.168
6      34.349392  LOCAL         *BROADCAST    ARP_RARP  ARP: Request, Target IP: 192.168.0.26

 +ETHERNET: Destination address : FFFFFFFFFFFF
 +ETHERNET: Source address : 002078114A62
  ETHERNET: Frame Length : 355 (0x0163)
  ETHERNET: Ethernet Type : 0x0800 (IP:  DOD Internet Protocol)
  ETHERNET: Ethernet Data: Number of data bytes remaining = 341 (0x0155)
-IP: ID = 0x5E1; Proto = UDP; Len: 341
  IP: Version = 4 (0x4)
  IP: Header Length = 20 (0x14)
  IP: Precedence = Routine
  IP: Type of Service = Normal Service
  IP: Total Length = 341 (0x155)
  IP: Identification = 1505 (0x5E1)
 +IP: Flags Summary = 0 (0x0)
  IP: Fragment Offset = 0 (0x0) bytes
  IP: Time to Live = 128 (0x80)
  IP: Protocol = UDP - User Datagram
  IP: Checksum = 0x33B8
  IP: Source Address = 0.0.0.0
  IP: Destination Address = 255.255.255.255
  IP: Data: Number of data bytes remaining = 321 (0x0141)
+UDP: IP Multicast: Src Port: BOOTP Client, (68); Dst Port: BOOTP Server (67); Length = 321 (0x141)

00000020  FF FF 00 44 00 43 01 41 7C 43 01 01 06 00 FB 0F     .D.C®A|C®®±.√☼

DHCP Protocol Request Message   F#: 4/34   Off: 42 (x2A)   L: 313 (x139)
```

Figure 3-4 DHCPRequest packet capture in Network Monitor

At this point, using information in the DHCP options field of the DHCPRequest packet, shown in Figure 3-5, the DHCP client requests a single IP address, DHCP: Requested Address = 192.168.0.26, for the DHCP: Host Name = win2kdc02 (the DHCP client's name). You can also see that the DHCP options field displays the IP address of the DHCP server as DHCP: Server Identifier.


Microsoft Network Monitor - [Capture: 1 (Detail)]
File Edit Display Tools Options Window Help

```
Frame  Time       Src MAC Addr  Dst MAC Addr  Protocol  Description                                   Src Oth
3      34.299320  3COM  C388A6  *BROADCAST    DHCP      Offer                   (xid=385F0FFB)        192.168
4      34.299320  LOCAL         *BROADCAST    DHCP      Request                 (xid=385F0FFB)        0.0.0.0
5      34.349392  3COM  C388A6  *BROADCAST    DHCP      ACK                     (xid=385F0FFB)        192.168
6      34.349392  LOCAL         *BROADCAST    ARP_RARP  ARP: Request, Target IP: 192.168.0.26
7      34.379435  LOCAL         *BROADCAST    ARP_RARP  ARP: Request, Target IP: 192.168.0.26
8      35.380875  LOCAL         *BROADCAST    ARP_RARP  ARP: Request, Target IP: 192.168.0.26
```

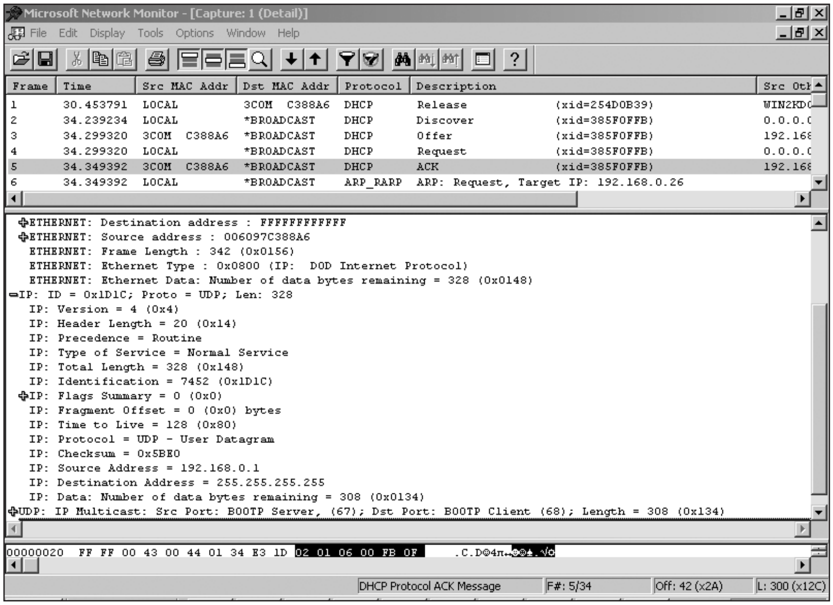
```
  DHCP: Seconds           (secs)   = 0 (0x0)
 +DHCP: Flags             (flags)  = 0 (0x0)
  DHCP: Client IP Address (ciaddr) = 0.0.0.0
  DHCP: Your   IP Address (yiaddr) = 0.0.0.0
  DHCP: Server IP Address (siaddr) = 0.0.0.0
  DHCP: Relay  IP Address (giaddr) = 0.0.0.0
  DHCP: Client Ethernet Address (chaddr) = 002078114A62
  DHCP: Server Host Name  (sname)  = <Blank>
  DHCP: Boot File Name    (file)   = <Blank>
  DHCP: Magic Cookie = 99.130.83.99
 -DHCP: Option Field      (options)
    DHCP: DHCP Message Type      = DHCP Request
    DHCP: Client-identifier      = (Type: 1) 00 20 78 11 4a 62
    DHCP: Requested Address      = 192.168.0.26
    DHCP: Server Identifier      = 192.168.0.1
    DHCP: Host Name              = win2kdc02
    DHCP: Dynamic DNS updates    = (Length: 13) 00 00 00 77 69 6e 32 6b 64 63 30 32 2e
    DHCP: Client Class information = (Length: 8) 4d 53 46 54 20 35 2e 30
    DHCP: Parameter Request List = (Length: 10) 01 0f 03 06 2c 2e 2f 1f 21 2b
    DHCP: End of this option field
```

```
00000110  00 00 00 00 00 00 63 82 53 63 35 01 03 3D 07 01   ......céSc5☺♥=•☺
```

Figure 3-5 DHCP options in the DHCPRequest packet

Step 4: DHCPAcknowledgment

The final step in the four-step DHCP process finds the DHCP server actually leasing the IP address to the client. Figure 3-6 shows the DHCPAck packet.


Microsoft Network Monitor - [Capture: 1 (Detail)]
File Edit Display Tools Options Window Help

```
Frame  Time       Src MAC Addr   Dst MAC Addr  Protocol  Description                                Src Oth
1      30.453791  LOCAL          3COM  C388A6  DHCP      Release             (xid=254D0B39)         WIN2KDC
2      34.239234  LOCAL          *BROADCAST    DHCP      Discover            (xid=385F0FFB)         0.0.0.0
3      34.299320  3COM  C388A6   *BROADCAST    DHCP      Offer               (xid=385F0FFB)         192.168
4      34.299320  LOCAL          *BROADCAST    DHCP      Request             (xid=385F0FFB)         0.0.0.0
5      34.349392  3COM  C388A6   *BROADCAST    DHCP      ACK                 (xid=385F0FFB)         192.168
6      34.349392  LOCAL          *BROADCAST    ARP_RARP  ARP: Request, Target IP: 192.168.0.26
```

```
 +ETHERNET: Destination address : FFFFFFFFFFFF
 +ETHERNET: Source address : 006097C388A6
  ETHERNET: Frame Length : 342 (0x0156)
  ETHERNET: Ethernet Type : 0x0800 (IP:  DOD Internet Protocol)
  ETHERNET: Ethernet Data: Number of data bytes remaining = 328 (0x0148)
-IP: ID = 0x1D1C; Proto = UDP; Len: 328
  IP: Version = 4 (0x4)
  IP: Header Length = 20 (0x14)
  IP: Precedence = Routine
  IP: Type of Service = Normal Service
  IP: Total Length = 328 (0x148)
  IP: Identification = 7452 (0x1D1C)
 +IP: Flags Summary = 0 (0x0)
  IP: Fragment Offset = 0 (0x0) bytes
  IP: Time to Live = 128 (0x80)
  IP: Protocol = UDP - User Datagram
  IP: Checksum = 0x5BE0
  IP: Source Address = 192.168.0.1
  IP: Destination Address = 255.255.255.255
  IP: Data: Number of data bytes remaining = 308 (0x0134)
+UDP: IP Multicast: Src Port: BOOTP Server, (67); Dst Port: BOOTP Client (68); Length = 308 (0x134)
```

```
00000020  FF FF 00 43 00 44 01 34 E3 1D 02 01 06 00 FB 0F     .C.D☺4π↔☻☺♠.√☼
```

```
DHCP Protocol ACK Message    F#: 5/34    Off: 42 (x2A)    L: 300 (x12C)
```

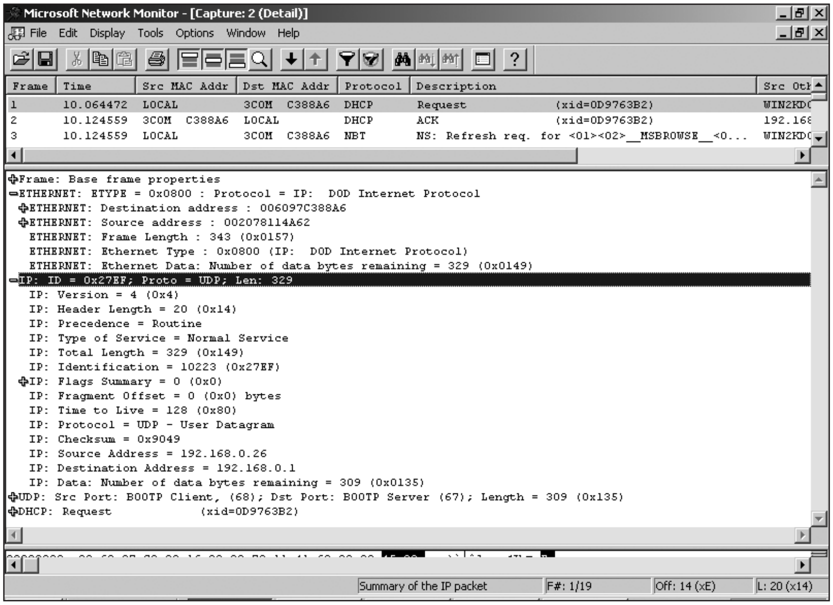
Figure 3-6 DHCPAcknowledgment packet capture in Network Monitor

The ETHERNET: Destination address is still the broadcast MAC Address. The ETHERNET: Source address is the MAC address of the DHCP Server. Also, because the client does not load and initialize TCP/IP until after it receives the DHCPAck, the IP: Destination Address remains the broadcast address 255.255.255.255. The IP: Source Address is the IP address of the DHCP Server. The client uses the IP: Source Address information to renew its lease after a certain time interval.

DHCP Renewal Process

DHCP clients use the entire four-step DHCP process to obtain their initial IP addresses or to renew an expired address. However, renewing an IP lease does not require all four steps. By default, halfway through their lease interval, all DHCP clients attempt to contact the DHCP server at the IP address specified in the DHCP options field for the DHCP: Server Identifier. For instance, eight days is the default lease for Windows 2000 DHCP servers. If this default lease is not changed, clients attempt to renew their IP addresses four days into the lease interval. If they cannot renew their leases, clients attempt again when 87.5% of the lease expires. Clients that cannot renew their leases with the original DHCP server (the one specified in the DHCP: Server Identifier) at the 87.5% interval, attempt to contact any DHCP server to renew their current lease. If their leases expire before they can renew their addresses, clients must complete the entire four-step process to get a new address. Administrators can manually renew a client's lease with the ipconfig /renew command.

Clients who successfully renew their leases halfway through the lease interval use a shorter, two-step process. They send a directed DHCP request to the DHCP server and the server responds with a DHCPAck. Figure 3-7 shows the DHCPRequest from a renewing client.



```
Frame  Time       Src MAC Addr   Dst MAC Addr   Protocol  Description                                    Src Oth
1      10.064472  LOCAL          3COM  C388A6   DHCP      Request              (xid=0D9763B2)            WIN2KDC
2      10.124559  3COM  C388A6   LOCAL          DHCP      ACK                  (xid=0D9763B2)            192.168
3      10.124559  LOCAL          3COM  C388A6   NBT       NS: Refresh req. for <01><02>__MSBROWSE__<0...   WIN2KDC
```

```
+Frame: Base frame properties
-ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
 +ETHERNET: Destination address : 006097C388A6
 +ETHERNET: Source address : 002078114A62
  ETHERNET: Frame Length : 343 (0x0157)
  ETHERNET: Ethernet Type : 0x0800 (IP:  DOD Internet Protocol)
  ETHERNET: Ethernet Data: Number of data bytes remaining = 329 (0x0149)
-IP: ID = 0x27EF; Proto = UDP; Len: 329
  IP: Version = 4 (0x4)
  IP: Header Length = 20 (0x14)
  IP: Precedence = Routine
  IP: Type of Service = Normal Service
  IP: Total Length = 329 (0x149)
  IP: Identification = 10223 (0x27EF)
 +IP: Flags Summary = 0 (0x0)
  IP: Fragment Offset = 0 (0x0) bytes
  IP: Time to Live = 128 (0x80)
  IP: Protocol = UDP - User Datagram
  IP: Checksum = 0x9049
  IP: Source Address = 192.168.0.26
  IP: Destination Address = 192.168.0.1
  IP: Data: Number of data bytes remaining = 309 (0x0135)
+UDP: Src Port: BOOTP Client, (68); Dst Port: BOOTP Server (67); Length = 309 (0x135)
+DHCP: Request             (xid=0D9763B2)
```

```
Summary of the IP packet    F#: 1/19    Off: 14 (xE)    L: 20 (x14)
```

Figure 3-7 DHCPRequest for a renewing client

Unlike the initial DHCPRequest packet, the DHCPRequest renewal packet has the client MAC address as the ETHERNET: Source Address and the DHCP server address as the ETHERNET: Destination Address. Also, the IP: Source Address is the IP address of the client. The IP: Destination Address is the IP address of the DHCP server. In short, instead of a broadcast, the DHPCRequest packet is now a directed message asking the DHCP server to renew the IP lease.

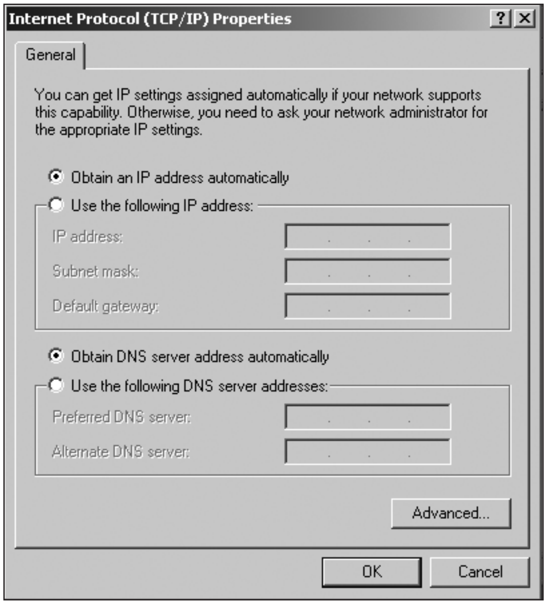
The server returns a DHCPAck if the client can continue to use the leased IP address. This packet is a directed message just like the DHCPRequest. It is possible that the DHCP server may issue a DHCPNack to the client. A DHCPNack occurs when the client has moved to another subnet, the range of addresses on the local subnet has changed, or the client's previous address has expired and was subsequently leased to another client.

CLIENT CONFIGURATION FOR DHCP

Any client that supports a standard implementation of DHCP can obtain an IP address from a Windows 2000 DHCP server. As long as a client follows the standards outlined in RFCs for a DHCP client, a Windows 2000 DHCP server can provide the client with a dynamic IP address.

Configuring Windows 2000 clients for use with DHCP was covered earlier in Chapter 2 in the section on TCP/IP.

To configure Windows clients, you must specify that they obtain an IP address automatically. In Windows 2000 you must access the Internet Protocols (TCP/IP) properties found under Local Area Connections properties. Figure 3-8 displays the internet protocols (TCP/IP) settings for a Windows 2000 machine configured as a DHCP client.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Figure 3-8 Windows 2000 machine configured as a DHCP client

Once configured, the client uses the four-phase DHCP process to obtain an IP address and the two-step renewal process to keep an IP address. On occasion, you may want to force a client to release a currently leased IP address or force it to renew its current IP lease. The ipconfig /release command issued after the command prompt forces a client to release its current dynamic IP address. The ipconfig /renew command forces the client either to renew the current lease, or if no lease is active, to start the lease process with a DHCPDiscover packet.

Sometimes a client cannot find a DHCP server when it issues a DHCPDiscover packet. This can occur because the DHCP server service on the DHCP server has stopped, the scope on the DHCP server has leased all available addresses, or the client is on a different broadcast domain than the DHCP server. When this happens to clients that had no previous lease, Window 2000 clients (and Windows 98 clients) implement **Automatic Private IP Addressing (APIPA)**. With APIPA, the client selects an address from the Class B network 169.254.0.0 with the default subnet mask 255.255.0.0. (Microsoft has reserved the

169.254.0.0 address as a private set of addresses with Internic, the organization that controls public IP addresses.) The client selects an address on the network 169.254.0.0 and then pings to see if any other device is using that address. If a client receives a successful ping reply, the client selects a different address. Each client tries up to 10 private addresses before it stops attempting to load IP. The client continues its attempts to contact a DHCP server every five minutes even though it has an APIPA. If it finds a DHCP server, the client accepts configuration information from the server and abandons the autoconfiguration information.

Windows 2000 clients that still have active leases at system start, but cannot find the DHCP server to renew their IP addresses, ping their default gateway. If the default gateway responds, the client assumes its current IP lease information is correct and continues to use it until it expires or the DHCP server renews it. If the default gateway does not respond, the client assumes it has been moved to another subnet and, because it cannot find a DHCP server, it performs APIPA as just described.

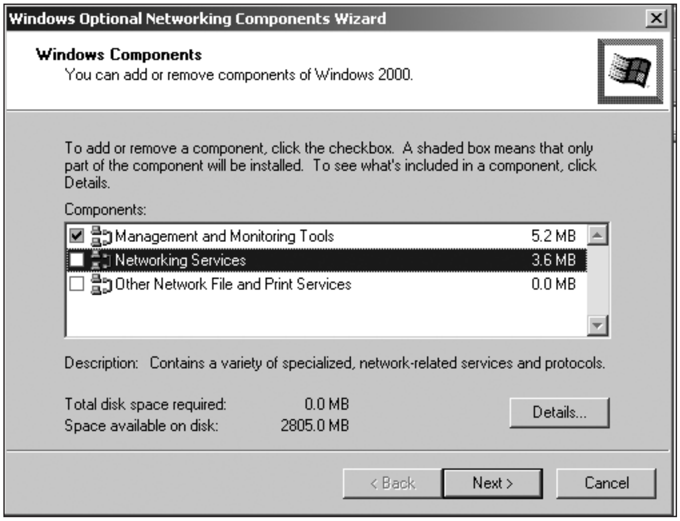
INSTALLING THE DHCP SERVER SERVICE

Installation of most networking services in Windows 2000 Server is not difficult. You must, however, make sure that your server meets the minimum requirements for each service. The DHCP server service requires the following:

- A Windows 2000 server machine configured with a static IP address, subnet mask, and, on networks with multiple subnets or networks, a default gateway
- A range of addresses that can be used to create scopes
- Active Directory installed and configured to allow DHCP servers to be authorized in AD

Although there are many ways to install DHCP, one of the easiest involves accessing Network and Dial-up Connections via the Start menu or by right-clicking on My Network Places and selecting Properties. Once in Network and Dial-up Connections on the server you wish to install DHCP, you must select the Advanced, Optional Networking Components item. This brings up the Windows Optional Networking Components Wizard shown in Figure 3-9.

You must select Networking Services and then click the Details button to open the Networking Services dialog box. To install the DHCP server service on your server, select Dynamic Host Configuration Protocol (DHCP), click the OK button, then click Next after you return to the Windows Optional Networking Components Wizard. You can manage the installed DHCP server service from the DHCP manager snap-in that is added to the Administrative Tools folder after installation. Figure 3-10 shows the DHCP manager snap-in.



Windows Components

You can add or remove components of Windows 2000.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

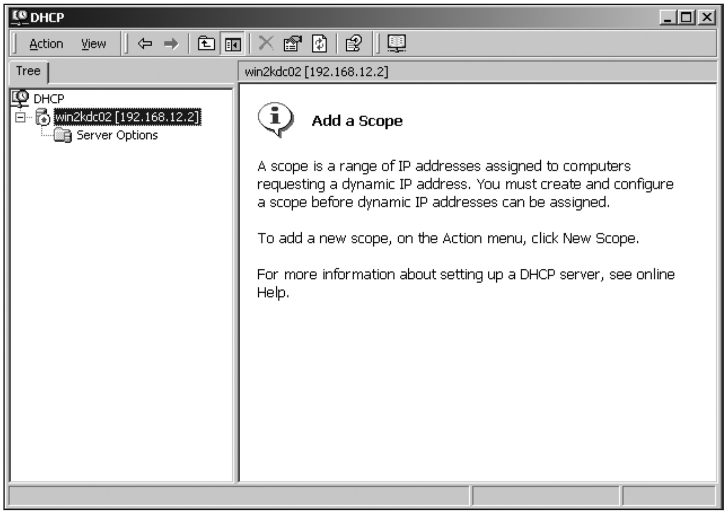
☑	Management and Monitoring Tools	5.2 MB
□	Networking Services	3.6 MB
□	Other Network File and Print Services	0.0 MB

Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 0.0 MB

Space available on disk: 2805.0 MB

Figure 3-9 Windows Optional Networking Components Wizard



Add a Scope

A scope is a range of IP addresses assigned to computers requesting a dynamic IP address. You must create and configure a scope before dynamic IP addresses can be assigned.

To add a new scope, on the Action menu, click New Scope.

For more information about setting up a DHCP server, see online Help.

Figure 3-10 DHCP Manager snap-in

The green up arrow next to the small server icon signifies that the DHCP server service is installed and currently running. You can also verify that the service is running by selecting Services under Administrative Tools. If the DHCP Server service Status is Started and its Startup Type is Automatic, you installed the service correctly. Installing the service is only part of the configuration necessary to plan successful DHCP services. As an administrator, you must also plan where to place your DHCP servers. Since all four phases of the initial DHCP lease process are broadcast-based, you must carefully plan placement of DHCP servers or implement **DHCP relay agents** or routers capable of forwarding DHCP broadcasts.

Figure 3-11 portrays a common problem on most networks attempting to implement DHCP. The problem occurs when a network consists of two Ethernet segments (or broadcast domains) connected by Router A. By default, routers do not pass broadcasts, so Router A discards any DHCPDiscover packets broadcast by the DHCP client. The client cannot contact a DHCP server; it uses APIPA to obtain an IP address. Unfortunately, that means that the client cannot use the services of Router A to access either the Internet or any other servers or machines out Router A's Ethernet0 (E0) interface.

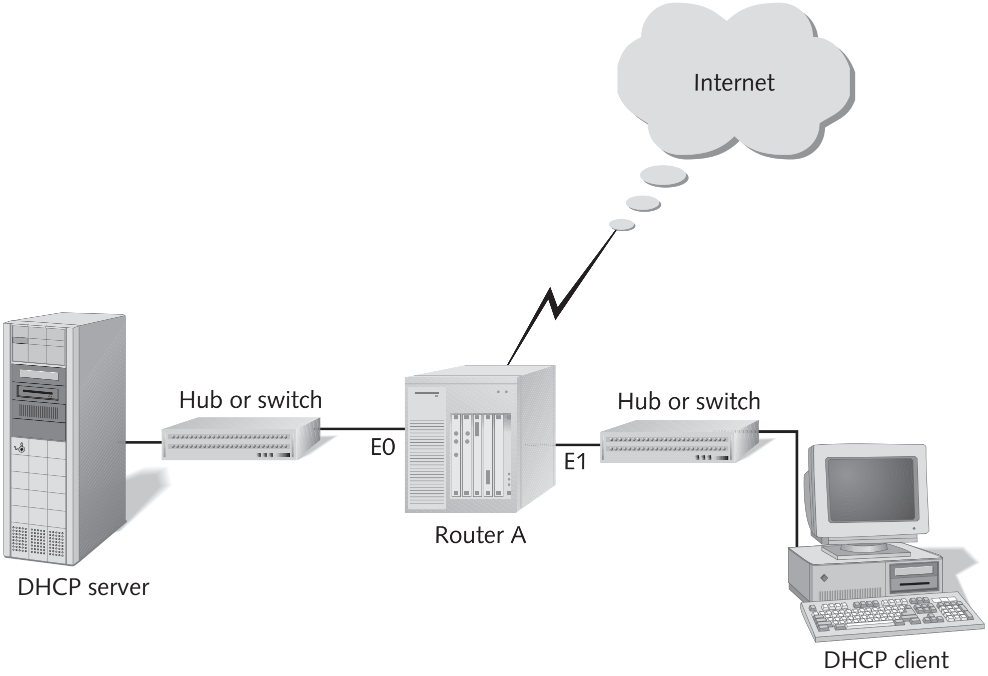


Figure 3-11 Router blocking DHCPDiscover packets

Configuring a Router to Pass DHCP Traffic

There are three ways to solve this problem. If the router supports it, it can be configured to allow DHCP traffic to pass. Most routers support the forwarding of DHCP broadcast traffic. Depending on the software installed on the router, Cisco routers allow DHCP traffic via the ip helper-address [*ip address of DHCP server*] command. Therefore, if the DHCP server in Figure 3-11 has the IP address 192.168.12.12, you use the ip helper-address 192.168.12.12 command to allow DHCP packets from the client to pass to the DHCP server. With this configuration, you would need only a single DHCP server configured with multiple scopes to support your DHCP clients. Unfortunately, the configuration also has a single point of failure—the single DHCP server. Regardless, many networks use this configuration to save server resources and to simplify management.

Configuring a DHCP Server per Physical Segment

Placing a second DHCP server on the same segment as the client is another way of solving this problem. While this method may seem extreme, it does limit the amount of traffic associated with DHCP that needs to pass through the router. Figure 3-12 shows a network with a DHCP server on each side of the router. The clients on each side can receive dynamic IP addresses from the DHCP server on the local segment. This solves the problem of broadcast traffic's inability to pass through the router.

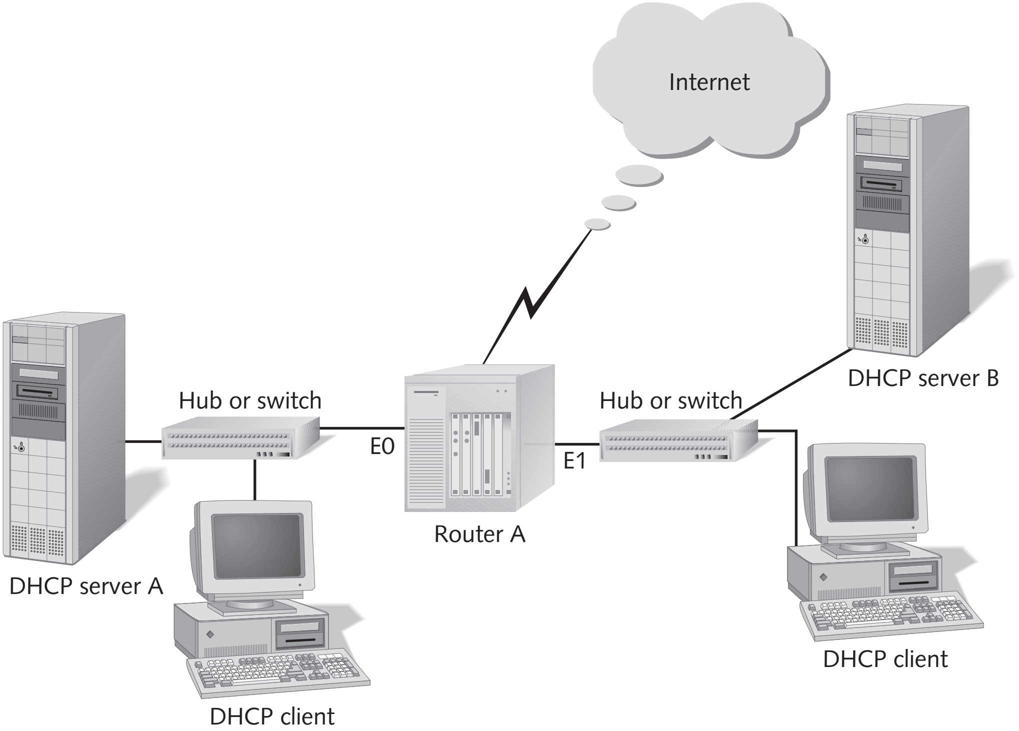
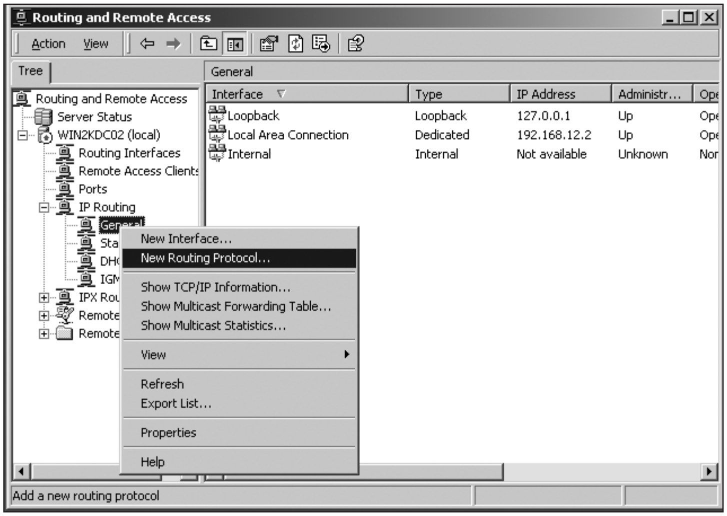


Figure 3-12 Multiple DHCP servers

You can use the same basic setup to create a fault-tolerant configuration for your DHCP servers. You can increase fault tolerance by creating two scopes on DHCP Server A. The first scope holds 75% of the available addresses for the local segment. The second scope holds 25% of the available addresses for the segment served primarily by DHCP Server B. Server B has a scope with 75% of its local available addresses and 25% of the addresses available on Server A's segment. Once you enable the router to pass DHCP traffic with the ip helper-address command on Cisco routers (or with similar commands on other manufacturers' routers), the two DHCP servers can provide addresses for their local clients, and, in the event one server fails, the remaining server provides addressing for the clients on the remote segment.

DHCP Relay Agents

The final way to solve the problem presented in Figure 3-11 is with a DHCP relay agent. A DHCP relay agent acts as a proxy for a DHCP server. If the DHCP relay agent sees a packet destined for a DHCP server, it grabs that packet and uses a directed message to the DHCP server that has been configured in its relay agent properties. It also receives packets sent back from the DHCP server and broadcasts those onto the local segment, so the DHCP clients can receive the DHCPOffer and DHCPAck packets. You must enable Routing and Remote Access services to configure a Windows 2000 machine as a DHCP relay agent. Once you do this, go to the local computer name listed in the Routing and Remote Access snap-in, expand the IP Routing item, right-click General, and then select New Routing Protocol. In the New Routing Protocol dialog box, select DHCP Relay Agent and click OK. This loads the DHCP Relay Agent. Figure 3-13 shows the New Routing Protocol item you must select to open the New Routing Protocol dialog box. Once configured, the relay agent begins forwarding DHCP packets.



Interface	Type	IP Address	Administr...	Ope
Loopback	Loopback	127.0.0.1	Up	Ope
Local Area Connection	Dedicated	192.168.12.2	Up	Ope
Internal	Internal	Not available	Unknown	Nor

Add a new routing protocol

Figure 3-13 New Routing Protocol

Note

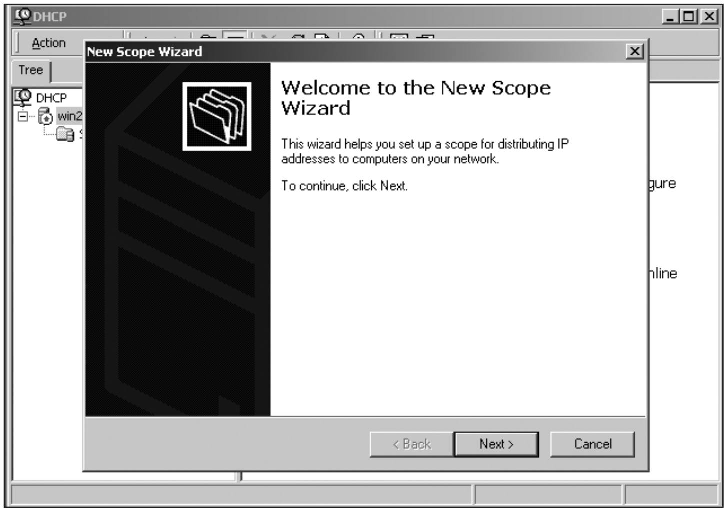
You cannot configure a Windows 2000 machine to run both the DHCP server service and the DHCP relay agent. Doing so results in erratic behavior by both networking components.

Configuring Scopes

After you correctly install the DHCP server service, you must create a scope of addresses for the server to dole out to clients.

For instance, if you have the Class C private network address of 192.168.12.0 with the default mask of 255.255.255.0, then you can configure a scope that consists of the entire usable range of addresses, 192.162.12.1 to 192.168.12.254, or any portion of these usable addresses. Normally, network administrators reserve some portion of usable addresses for machines that require static IP addresses. In a Class C network, you will probably want to create scopes that do not include the first twenty or so usable IP addresses. Then you can use these addresses for static clients. Although the exclusion feature lets you exclude certain IP addresses from scopes, it is much easier to simply remove a portion of your IP addresses from the scope before creating it.

To begin creating a scope, you must open the DHCP manager snap-in found in the Administrative Tools folder on the Start menu, right-click the server name, and then select New Scope. Figure 3-14 shows the New Scope Wizard that appears when you select New Scope.



Welcome to the New Scope Wizard

This wizard helps you set up a scope for distributing IP addresses to computers on your network.

To continue, click Next.

Figure 3-14 Creating a new scope in the DHCP manager snap-in

The New Scope Wizard then walks you through the steps of creating a new scope. Specifically, the wizard prompts you for the following items:

- *Name and Description*: The name of the scope as it will appear in the DHCP Manager and a short description of the scope
- *IP Address range*: The range of addresses to be leased to clients
- *Subnet mask*: The subnet mask information for the scope. The recommendation for Windows 2000 is a subnet mask based on the class of the addresses placed in the IP address range. If you have custom subnet masks (that is, you are subnetting), then you can specify the subnet mask in bits or with a decimal equivalent.

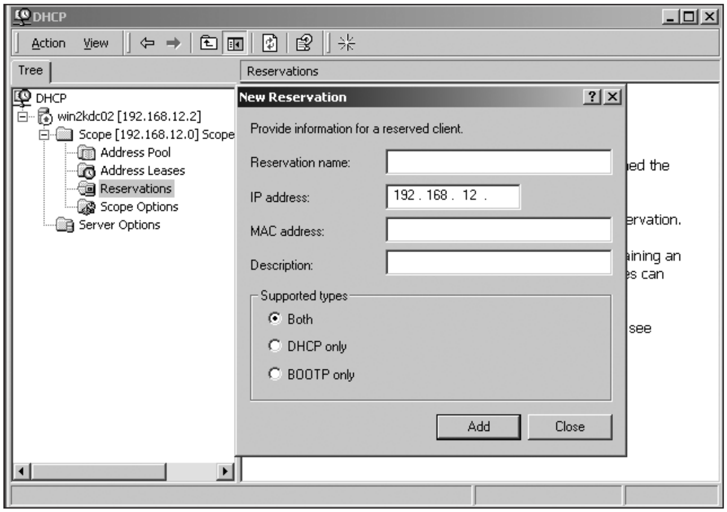
- *Add Exclusions*: At this point, you can exclude any addresses in the IP address range that you do not want dynamically leased to clients. However, it is better to place only the IP addresses that you want leased in the IP address range. That way, you do not need to add any exclusions.
- *Lease duration*: You can either accept the default lease duration of eight days or change it to a value more suitable for your network. If you constantly move computers from one subnet to another or if you are in danger of running out of IP addresses, you may want to shorten the lease for a scope to three days (the old Windows NT DHCP default lease duration) or less. If your network clients rarely change subnets and you have abundant IP addresses, increasing the DHCP lease duration lessens the network traffic created by DHCP renewals.
- *Configure DHCP Options*: The final question the New Scope Wizard asks is if you want to configure scope options. **Options** are extra configuration information such as default gateway, DNS server, and WINS server addresses that you can give to a DHCP client when clients lease an IP address. The section, "Scope Options," later in this chapter, provides greater detail.

The Windows 2000 DHCP server service also supports providing multicast addresses to clients via DHCP. The process of creating a multicast scope is very similar to creating a normal scope. To create a multicast scope, you right-click on the server name in DHCP manager snap-in and select New Multicast Scope. The New Multicast Scope Wizard then walks you through the process of creating a multicast scope.

Finally, superscopes are available to allow grouping and management of multiple scopes as one unit. This allows administrators to assign multiple IP ranges to a single physical subnet or to group scopes together for easier management. Superscopes allow administrators to expand a physical segment beyond its initial limit of one range of addresses. For instance, an administrator may assign a single Class C address range for a physical segment. That segment may grow beyond the 254 hosts allowed for a single Class C range of addresses. With superscopes, the administrator can group two Class C ranges together to serve a single physical segment.

Another common use of superscopes involves the process of migrating to a new range of dynamic IP addresses. You can use superscopes to configure and manage both ranges during the transition process. Combining multiple member scopes together creates superscopes. **Member scopes** are just normal scopes placed within a superscope. To create a superscope, you create the scopes you want to include in the superscope, then you right-click the server name in DHCP Manager and select New Superscope. The New Superscope Wizard allows you to group multiple scopes into a superscope.

On occasion, you may want to reserve a specific IP address for a specific client. In effect, **reservations** allow you to assign one particular IP address in the scope to a single client. You configure reservations in the Reservations folder under a particular scope. Right-click the Reservations folder and select New Reservation to open the New Reservation dialog box shown in Figure 3-15.



Provide information for a reserved client.

Reservation name:

IP address: 192 . 168 . 12 .

MAC address:

Description:

Supported types

● Both

○ DHCP only

○ BOOTP only

Figure 3-15 Configuring a client reservation

You must specify a Reservation name, an IP address in the scope, and the MAC address of the client for which you want a reservation. You may include an optional description. You can also select if this reservation is for DHCP, BootP, or both.

BootP is the method that diskless workstations originally used to obtain IP addresses from BootP servers. The specifications for DHCP borrowed from the old BootP methods. Windows 2000 supports BootP clients to provide backward compatibility.

If you do not know the MAC address of the client, obtain it by running the ipconfig /all command from the command prompt.

Scope Options

Once you install the DHCP server service and create your scopes, it is time to specify options. Options are additional parameters that you can configure for clients using dynamic IP addresses. You can configure options globally for all scopes (for such items as DNS servers or WINS servers), for a single scope (for such items as default gateways), for a vendor-defined or user-defined class, or on a reserved client basis. You configure most options at the **scope options** or **server options** level. **Vendor-defined option classes** and **user-defined option classes** are available for clients that need special configuration parameters. Use them only if no other means are available for assigning an option. **Reserved client options** allow you to give a specific configuration to a client with a reservation. Again, whenever possible, try to use server and scope options. Table 3-1 describes the main options used with DHCP.

Table 3-1 DHCP options

Option	Parameter	Function
003 Router	IP address of default gateway	Provides clients with IP address of default gateway on their local network segment
006 DNS servers	IP addresses of DNS servers on network	Provides clients with IP address of DNS servers on their network
015 DNS Domain Name	Domain name for network; for example, course.com or microsoft.com	Provides clients with DNS domain name of their network
044 WINS/NBNS server	IP address of WINS server(s) on network	Provides clients with IP address of WINS servers on their network; setting this option automatically adds the 046 WINS/NBT Node Type option to your scope options
046 WINS/NBT Node Type	0x1: broadcast node 0x2: point-to-point node 0x4: mixed-node 0x8: hybrid mode (the section on WINS discusses each of these in detail)	Provides clients with a NetBIOS Node Type; although four settings are possible you should always set 046 to 0x8.

Configuring options is a very simple procedure. To configure global options, you navigate to Administrative Tools on the Start menu and select DHCP to start the DHCP manager snap-in. Once it loads, you right-click the Server Options folder and select Configure Options. All options created under the Server Options folder are server and apply to all scopes on the DHCP server. You use server options for items such as DNS servers and WINS servers, items that are the same for all clients in all scopes.

You must right-click the Scope Options folder for a particular scope in order to set scope options. Once you select Configure Options, you can configure options for a particular scope. Also, under the Advanced tab in scope options or server options, you can select and define vendor-defined option classes and user-defined option classes.

Configuring reserved client options requires that you first create a client reservation. Then you can right-click the reservation and select Configure Options to set the required options.

DHCP AND ACTIVE DIRECTORY

Rogue DHCP server detection is one of the most important new features of the Windows 2000 DHCP server service. If Active Directory is installed and configured correctly on your network, you can create a DHCP object within AD to validate DHCP servers. When a DHCP server comes online and registers with Active Directory, its IP address is checked against the authorized DHCP servers. If its IP address is not one of the authorized servers, the DHCP service stops and the server cannot answer the client request. Integrating DHCP server with Active Directory requires that all DHCP servers run Windows 2000 (Windows NT DHCP servers cannot be authorized in the AD) and that the first DHCP server in your network is installed as either a domain controller or member server. To authorize a Windows 2000 DHCP server, you must first login as an Enterprise Administrator or with a user account that has the right to add DHCP servers to your Active Directory. Then follow these steps:

1. Open the **DHCP manager snap-in** under Administrative Tools
2. Click the **Action** menu and select **Manage Authorized Servers**
3. Click the **Authorize** button and type the **IP address of the Windows 2000 DHCP server** you want to authorize
4. Click **OK** to close the dialog box

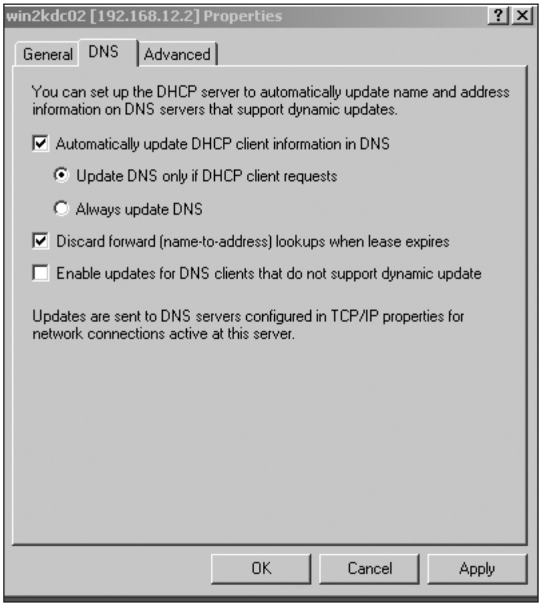
If Active Directory is not loaded, an error message appears, stating that the Active Directory cannot be found. Without Active Directory properly loaded, you cannot authorize DHCP servers, and rogue DHCP server detection is not available.

INTEGRATING DHCP AND DNS

The Domain Name System server that ships with Windows 2000 supports dynamic updates of both A records and pointer (PTR), also known as **reverse lookup records**. In fact, the DHCP server service that ships with Windows 2000 can act as a proxy for clients that do not support dynamic DNS updates. Using this feature of DHCP ensures that clients receiving dynamic IP addresses have the correct information stored in the DNS database. Before DHCP can act as a proxy, you must enable DNS to allow updates for non-dynamic DNS aware clients. You accomplish this task in the DNS snap-in with the Properties command on the Action menu. If you select Enable Updates for DNS Clients that Do Not Support Dynamic Update, the DHCP server can dynamically register non-DDNS aware clients with the DNS service.

Of course, you must also configure your DHCP server to act as a proxy. Figure 3-16 displays the DNS tab that you see when you right-click the DHCP server in the DHCP snap-in and select Properties.

To enable the DHCP server to dynamically register all clients, select the Always update DNS radio button and check the item, Enable updates for DNS clients that do not support dynamic update. These two options force the DHCP server to register both A records (host name to IP address mappings) and pointer (PTR) or reverse lookup (PTR) records (IP address to host name mappings) with the DNS server.



You can set up the DHCP server to automatically update name and address information on DNS servers that support dynamic updates.

☑ Automatically update DHCP client information in DNS

● Update DNS only if DHCP client requests

○ Always update DNS

☑ Discard forward (name-to-address) lookups when lease expires

□ Enable updates for DNS clients that do not support dynamic update

Updates are sent to DNS servers configured in TCP/IP properties for network connections active at this server.

Figure 3-16 DHCP DNS configuration tab

Note

Windows 2000 clients support registering their own A records via dynamic DNS updates. They do, however, rely on the DHCP server to register their PTR records with the DNS server.

MANAGING, MONITORING, AND TROUBLESHOOTING DHCP

Many tools are available for managing, monitoring, and troubleshooting DHCP. In this section you explore some of these tools and learn how to perform basic troubleshooting.

Managing DHCP

Throughout this chapter on DHCP, the DHCP snap-in has been your main tool for managing DHCP. During real-world, day-to-day administration, this is the tool you use to create scopes, manage options, and configure most DHCP settings. There are, however, other tools for managing DHCP.

One management task you may need to perform is to stop the DHCP service.You can accomplish this task in several ways. First, you can open the DHCP snap-in, then click Action, All Tasks, Stop. From the command prompt, you can stop the DHCP server service with the net stop dhcpserver command. Likewise, you can restart the DHCP server service from the command prompt with the net start dhcpserver command. It is also possible to start and stop the DHCP server using the Services snap-in found under Administrative Tools. You must locate the DHCP server service and then click the Stop button to shut down the service.

Compacting the DHCP database with the jetpack command is a fairly uncommon but essential administrative task in certain circumstances. The DHCP database resides in the systemroot\winnt\system32\dhcp directory in a file named dhcp.mdb. If the file dhcp.mdb is 30 MB or larger in size, you probably need to run the jetpack utility on the database. Running the utility requires three steps:

1. Stop the **DHCP server service** from either the DHCP snap-in or the command line with the net stop dhcpserver command.
2. From the command prompt, navigate to the systemroot\winnt\system32\dhcp directory, and run the following command: jetpack dhcp.mdb temp.mdb. (The second database name can be anything; .mdb is a temporary database used only during the jetpack process.)
3. Restart the **DHCP server service**.

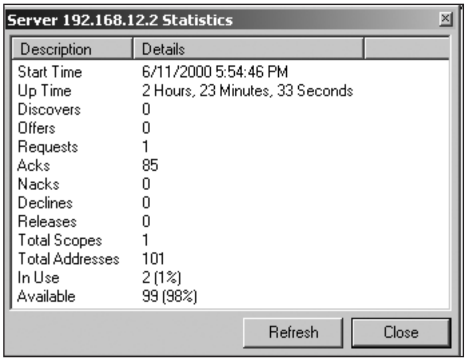
Managing DHCP also means managing DHCP clients. The easiest way to retrieve configuration information from a client is the ipconfig /all command issued at the command prompt. This command displays all information concerning a client's DHCP configuration. You can use the ipconfig /release and ipconfig /renew commands to force a client to release its lease and renew its lease. This is useful if you change the scope of addresses on a network and want all clients to obtain IP addresses in the new range.

Moving the DHCP database to a different DHCP server, dhcp.mdb, is one task you may need to perform if you upgrade to a newer machine or if you need to remove a DHCP server from the network for maintenance. The steps for moving a DHCP database are very simple. First, you must stop the DHCP server service on both computers using one of the methods described earlier in this section. The easiest method is the net stop dhcpserver command issued after the command prompt. You must then copy the entire contents of the systemroot\winnt\system32\dhcp folder to exactly the same path on the new computer. It is possible to move the database to a new directory, but you should not copy the .log or .chk files to the new directory. Finally, you should restart the DHCP service on the new computer. On both computers you should also click on the server, select Action, and then select Reconcile All Scopes.

Monitoring DHCP

DHCP monitoring is like DHCP management: you can perform it with many different tools. Basic monitoring is available within the DHCP snap-in by clicking on a particular server and then selecting Action, Display Statistics. Figure 3-17 displays the statistics available within the DHCP snap-in.

These basic statistics allow you to quickly view server uptime, numbers of available addresses, and the number of leased addresses.

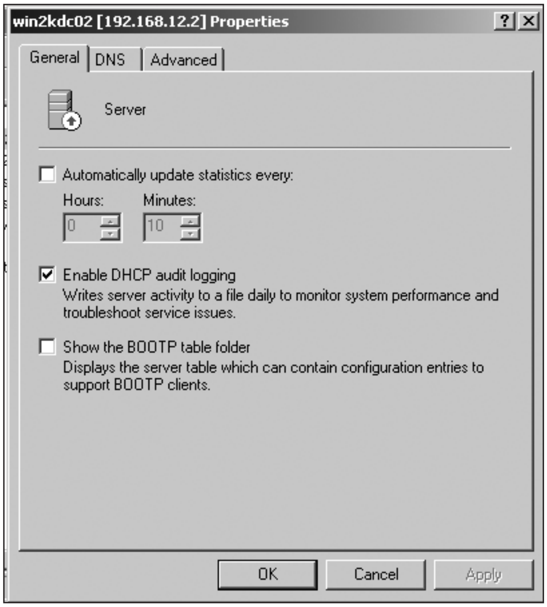


Server 192.168.12.2 Statistics

Description	Details
Start Time	6/11/2000 5:54:46 PM
Up Time	2 Hours, 23 Minutes, 33 Seconds
Discovers	0
Offers	0
Requests	1
Acks	85
Nacks	0
Declines	0
Releases	0
Total Scopes	1
Total Addresses	101
In Use	2 (1%)
Available	99 (98%)

Figure 3-17 DHCP statistics within DHCP snap-in

In addition to these basic statistics, the Windows 2000 DHCP server service can write a daily log of DHCP activity. This log is stored in the systemroot\winnt\system32\dhcp folder. This is a daily log saved as DhcpSrvLog.sun. The extension corresponds to the day of the log. For example, a Saturday log has the same name, DhcpSrvLog, but a different extension, .sat. You can configure some aspects of this logging activity within the DHCP snap-in. If you select a server in the snap-in, click Action, and then select Properties, you see the Properties dialog box for that particular server. On the General tab shown in Figure 3-18, you can enable or disable the DHCP audit log. It is enabled by default. On the Advanced tab shown in Figure 3-19, you can set the path to the audit logs.



win2kdc02 [192.168.12.2] Properties

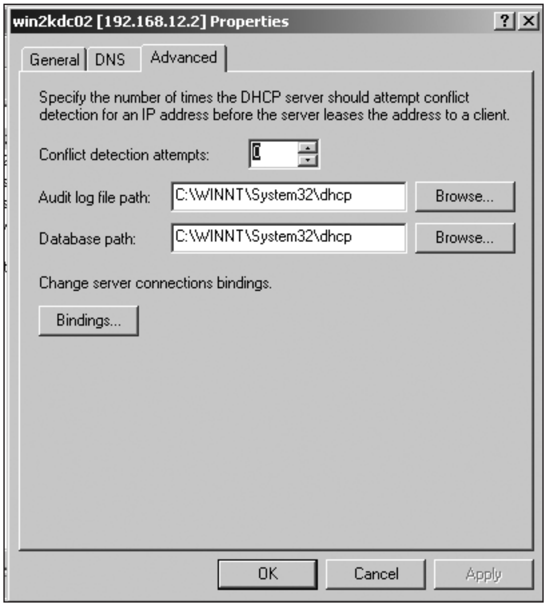
□ Automatically update statistics every:

Hours: 0 Minutes: 10

☑ Enable DHCP audit logging
Writes server activity to a file daily to monitor system performance and troubleshoot service issues.

□ Show the BOOTP table folder
Displays the server table which can contain configuration entries to support BOOTP clients.

Figure 3-18 General properties tab for a DHCP Server



Specify the number of times the DHCP server should attempt conflict detection for an IP address before the server leases the address to a client.

Conflict detection attempts: 0

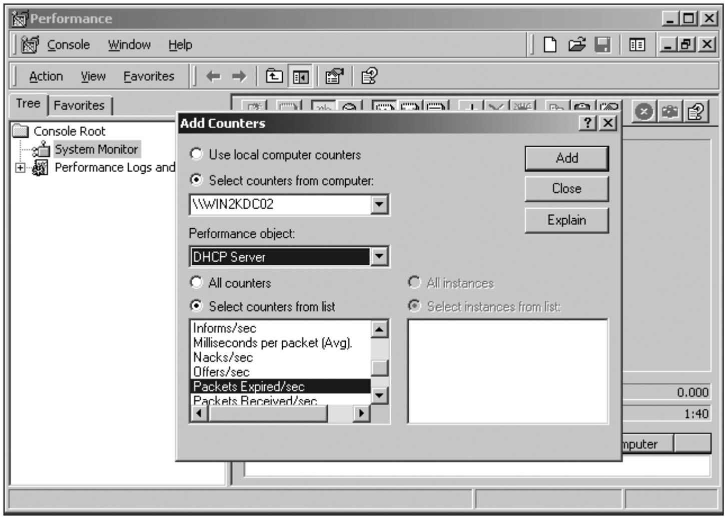
Audit log file path: C:\WINNT\System32\dhcp

Database path: C:\WINNT\System32\dhcp

Change server connections bindings.

Figure 3-19 Advanced properties tab for a DHCP Server

Using System Monitor is probably the most powerful and effective way to monitor DHCP server performance. Once you install the DHCP server service on a Windows 2000 server, new counters are added to System Monitor to allow detailed monitoring. You can access System Monitor from the Performance snap-in located in Administrative Tools. Once started, selecting the System Monitor and right-clicking in the chart area on the right allows you to select from the multitude of DHCP performance counters shown in Figure 3-20.



○ Use local computer counters

● Select counters from computer:

\\WIN2KDC02

Performance object:

DHCP Server

○ All counters

● Select counters from list

Informs/sec
Milliseconds per packet (Avg).
Nacks/sec
Offers/sec
Packets Expired/sec
Packets Received/sec

○ All instances

● Select instances from list:

Figure 3-20 System Monitor counters for DHCP

The DHCP Server Performance Object under System Monitor provides multiple counters that you can use to monitor your DHCP server performance. Discovers/sec, Offers/sec, Requests/sec and Acks/sec are all counters that allow you to see exactly how much DHCP traffic your server must handle. If the workload becomes excessive, you may need to add additional DHCP servers.

Troubleshooting DHCP

Most problems with DHCP involve misconfigured scopes or options, a stopped DHCP server service, a scope that has run out of addresses, or an improperly configured network.

Misconfigured scopes and options normally result from simple typos by the network administrator. If you suspect that a client is receiving incorrect option information, use the ipconfig /all command to verify client settings and information. Many times the incorrectly configured option is readily apparent in the DHCP client configuration information. Once you know what has been incorrectly set, you can change the options within the DHCP snap-in.

If a DHCP server does not respond to client requests and clients use APIPA to obtain IP addresses, you may have a stopped DHCP server service. As mentioned previously, the net start dhcpserver command should fix this problem quickly.

Sometimes, a scope runs out of addresses to lease. When this occurs, Windows 2000 clients use APIPA to complete their IP configurations. This can cause a multitude of network communication problems. Fixing this problem is not as simple or straightforward as solving other problems discussed in this section. Decreasing the length of lease for the scope is one possible solution to this problem. If more addresses are available, you may be able to increase the range of addresses in the scope. Final possible answers are renumbering the entire scope with a new and larger range of addresses or removing some clients from the overcrowded network segment.

Other problems with DHCP have nothing to do with the configuration of the client or the server. Instead, they may result from poor network design. As mentioned earlier, all four steps of the DHCP process use broadcast extensively. If any network device that blocks broadcast separates the DHCP clients and DHCP servers, the DHCP process fails.

If a DHCP client cannot send UDP broadcast to the DHCP server, it cannot obtain an IP address. To fix this problem, you must either place a DHCP server on each subnet or implement DHCP relay agents on subnets without DHCP servers.

Chapter Summary

- The dynamic host configuration protocol provides an easy way for network administrators to provide IP addressing information for network clients. Instead of visiting each client to configure a static IP address, network administrators can use the Windows 2000 DHCP server service to create a pool of IP addresses known as scopes that can be dynamically assigned to clients.

- Clients use a four-step process when initially leasing an IP address via DHCP. You can easily remember the four steps, **D**iscover, **O**ffer, **R**equest, **A**cknowledgment, by thinking of the sentence. "Aunt **DORA** helps with IP addressing."

- Configuring a Windows 2000 server with the DHCP server service includes the following steps:

  1. Configuring a static IP address, subnet mask, and default gateway on the server
  2. Installing the DHCP server service
  3. Creating scopes and, if needed, multicast scopes and superscopes
  4. Creating and specifying options on a server, scope, vendor-defined, user-defined, or reserved client basis (most options are server and scope)
  5. Authorizing the DHCP server in Active Directory

- DHCP in Windows 2000 is tightly integrated with the new Dynamic DNS features. You can configure DHCP to create DDNS entries for clients that do not support DDNS. This feature helps with support of legacy, non-DDNS aware clients. Windows 2000 clients can register their own A records, but they still rely on the DHCP server to create reverse lookup records.

- Finally, myriad tools are available for managing, monitoring, and troubleshooting DHCP. The final section of this chapter discusses many of these tools.

KEY TERMS

Automatic Private IP Addressing (APIPA) — New feature in Windows 98 and Windows 2000 that allows DHCP clients to select an IP address from the private range 169.254.0.0/16 whenever they cannot find a DHCP server on the local segment.

A records — Host name to IP address mappings in the DNS database that are used in host name resolution.

BootP — Older alternative to DHCP that diskless workstations used to obtain IP addresses.

broadcast domain — That portion of a network where broadcasts are propagated; normally broadcast domains are created by router placement in a network.

DHCPAcknowledgment — Packet broadcast by a DHCP server to a DHCP client that grants the client a lease for a particular IP address; fourth step of four-step DHCP lease process.

DHCPDiscover — Packet broadcast by DHCP clients to find DHCP servers on the local segment; first step of four-step DHCP lease process.

DHCPNack — Negative acknowledgment that a DHCP server broadcasts if it must decline a client's request for a particular IP address.

DHCPOffer — Packet broadcast by a DHCP server to a DHCP client that contains a possible IP address for lease; second step of four-step DHCP lease process.

DHCP relay agent — Software component loaded via Routing and Remote Access Service to a Windows 2000 machine; allows a machine to act as a proxy for DHCP clients on a segment.

DHCPRequest — Packet broadcast by a DHCP client requesting the IP address offered in a DHCPOffer packet; third step of four-step DHCP lease process.

Dynamic Domain Name System (DDNS) — Extension to the DNS systems that allows dynamic updates to the DNS database. The Windows 2000 DHCP server service can integrate with DDNS to allow dynamic DNS registration for clients that receive dynamic IP addresses.

Media Access Control (MAC) address — Physical address burned in the EPROM on a network card when it is manufactured.

member scopes — Scopes joined together in superscopes.

Microsoft Management Console (MMC) — Extensible framework within which Windows 2000 management snap-ins such as the DHCP snap-in reside.

multicast scopes — Ranges of multicast addresses configured to be dynamically assigned to host via DHCP.

options — Extra IP configuration parameters that can be given to DHCP clients when they lease an IP address.

pointer (PTR) resource records — Map an IP address to a fully qualified domain name (FQDN). *See also* reverse lookup records.

Reserved client options — Scope options created for a single client that has been given a DHCP reservation.

reverse lookup records — Another name for PTR records. These records resolve a host name from a known IP address.

reservations — Using the MAC address of the client to ensure that a particular IP address is always leased to that client.

scope options — Options that apply to all clients in one scope only.

scopes — Ranges of IP addresses configured for lease to clients via DHCP.

server options — Options that apply to all clients in all scopes configured on a DHCP server.

superscopes — Multiple scopes grouped together to allow centralized management; also allow for more than one range of IP addresses on a single physical subnet.

user-defined option classes — Allow expansion of DHCP options to include parameters determined by the network administrator for a particular client.

vendor-defined option classes — Expanded DHCP options created for one particular vendor's computers or network hardware.

Review Questions

1. Which of the following steps does a DHCP client perform in the DHCP lease process? (Choose all that apply.)
   a. DHCPOffer
   b. DHCPDiscover
   c. DHCPNack
   d. DHCPRequest

2. What scope option allows you to define the default gateway for DHCP clients?
   a. 044
   b. 003
   c. 006
   d. 015
3. Which of the following are advantages of using DHCP on your network? (Choose all that apply.)
   a. Easier IP address management
   b. Elimination of all static IP addresses
   c. Reduction in server load due to less network services being needed
   d. Leasing of options such as DNS server, WINS server, and Domain Name
4. A ________________ is a range of IP addresses that DHCP clients can lease.
5. All four steps in the DHCP lease process are sent to the broadcast IP address 255.255.255.255. True or false?
6. What does combining multiple scopes together for administrative purposes create?
   a. Multicast scopes
   b. Superscopes
   c. Big area scopes
   d. DHCP relay agents
7. A DHCP server requires a static IP address, subnet mask, and default gateway. True or false?
8. At what interval do clients attempt to initially renew their lease?
   a. Once every 24 hours
   b. Every 5 minutes
   c. 87.5 percent of the lease interval
   d. One-half the lease interval
9. Which one of the following can forward DHCP packets to a DHCP server on a different network segment?
   a. DHCP Server Agent
   b. DHCP Relay Agent
   c. DHCP DNS Agent
   d. DHCP Broadcast Agent

10. When you install DHCP, counters are added to facilitate monitoring in which one of the following?
    - a. Performance Monitor
    - b. DHCP snap-in
    - c. System Monitor
    - d. Active Directory

11. You can configure the DHCP server to create ________________ records and pointer (PTR) records for hosts that do not support DDNS.

12. Which of the following commands stops the DHCP server service?
    - a. net start dhcpserver
    - b. net stop dhcp
    - c. net stop dhcp snap-in
    - d. net stop dhcpserver

13. Which one of the following new features of the Windows 2000 DHCP server service stops inappropriate leasing of IP addresses from unauthorized DHCP servers?
    - a. Rogue DHCP server detection
    - b. DHCP validation and reconfiguration via DDNS
    - c. Superscopes
    - d. DHCP and DNS integration

14. If you configure the 044 WINS/NBNS server option for a scope, which one of the following options **must** you configure?
    - a. 003
    - b. 046
    - c. 005
    - d. 006

15. Your DHCP database is over 30 MB, and clients have trouble getting fast response from the DHCP server. Which one of the following commands should you run to fix the problem?
    - a. ipconfig /renew
    - b. jetpack
    - c. ipconfig /release
    - d. None, just reinstall DHCP

16. A DHCP client has problems attaching to network resources. You run the ipconfig command and find that the client's IP address is 169.254.12.4. What is the most likely reason your client has this Class B address?
    a. The client was unable to find a DHCP server and used APIPA to configure TCP/IP.
    b. The DHCP server is configured to give out addresses in the 169.254.0.0 range.
    c. The client has been assigned 169.254.12.4 as a static address.
    d. Because of an address conflict between this client and another client, the client used APIPA to configure TCP/IP.
17. A DHCP server performs which of the following steps in the DHCP lease process? (Choose all that apply.)
    a. DHCPOffer
    b. DHCPDiscover
    c. DHCPNack
    d. DHCPRequest
18. If they support DHCP broadcast forwarding, routers can be used instead of DHCP relay agents on networks with a single DHCP server and multiple physical network segments. True or false?
19. To authorize a DHCP server in Active Directory, what must you log in as? (Choose all that apply.)
    a. Enterprise Administrator
    b. Server Operator
    c. Local Administrator
    d. An account that has the right to authorize DHCP servers
20. Which one of the following creates and stores a daily log of DHCP activity?
    a. DHCP snap-in
    b. DHCP activity log
    c. System Monitor
    d. Active Directory

HANDS-ON PROJECTS

All Hands-on Projects in this chapter require two computers set up, as described in the lab set-up section in the front of this book. For these exercises, you use the PCs named win2kpro1 and win2kdc02. To complete these exercises, you must have completed Hands-on Projects 2-1 and 2-2 on the machine named win2kdc02.

Project 3-1

To install Active Directory so the DHCP server can be authorized in AD:

1. Click **Start** and then select **Run**.
2. In the Run dialog box, type **dcpromo**.
3. In the Active Directory Installation Wizard dialog box, click **Next**.
4. Select the **Domain controller for a new domain** radio button, and then click **Next** to continue.
5. Select the **Create a new domain tree** radio button, and then click **Next** to continue.
6. Select **Create new forest of domain trees**, and then click **Next** to continue.
7. In the Full DNS name for new domain: box, type **win2kclass02.org**, and click **Next**.
8. Click **Next** to accept the default NetBIOS Domain Name.
9. Click **Next** to accept the default Database and Log locations.
10. Click **Next** to accept the default Shared System Volume location.
11. Click **OK** to close the Active Directory Installation Wizard concerning DNS.
12. Select the **Yes, install and configure DNS on this computer (recommended)** radio button, and then click **Next** to continue.
13. Click **Next** to accept the default Permissions settings.
14. Type **password** in the Password and Confirm password boxes for the Directory Services Restore Mode Administrators Password, and click **Next**.
15. Click **Next** on the Summary page to continue.
16. Click **Finish** to close the Active Directory Installation Wizard.
17. Click **Restart Now** to restart the system and load Active Directory.

Project 3-2

To install the DHCP server service on the domain controller win2kdc02:

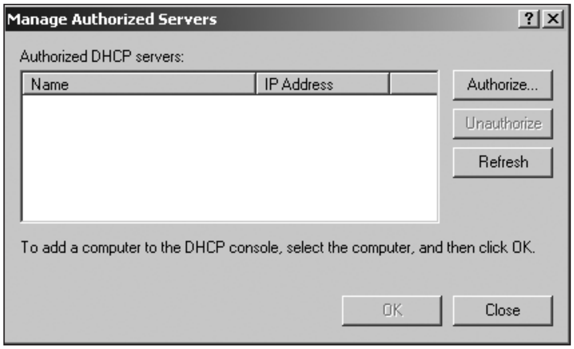
1. Click **Start**, **Settings**, **Network and Dial-up Connections**.
2. In Network and Dial-up Connections, click **Advanced** and then click **Optional Networking Components**.
3. Double-click **Networking Services** to see a list of networking services you can install.
4. Click in the box beside **Dynamic Host Configuration Protocol (DHCP)** to select the DHCP server service.
5. Click **OK** to close the Networking Services dialog box.
6. Click **Next** to complete installation of the DHCP server service.

Project 3-3

This project requires you to log in as Administrator. (This account is a member of the Enterprise Administrator's group by default.)

To authorize a DHCP server in Active Directory:

1. Click **Start**, **Programs**, **Administrative Tools**, **DHCP**.
2. In the DHCP snap-in, click **Action** and then click **Manage Authorized Servers**. The Manage Authorized Servers dialog box shown in Figure 3-21 appears.



To add a computer to the DHCP console, select the computer, and then click OK.

Figure 3-21 Manage Authorized Servers dialog box

3. Click the **Authorize** button and type the **IP address** of your server. (From the command prompt, use the ipconfig /all command to determine your server IP address.) Click **OK**.
4. Click **Yes** in the informational dialog box concerning adding the server to the authorized list.
5. Click **Close** to close the Manage Authorized Servers dialog box.

   You authorized your server as a DHCP Server within Active Directory.

Project 3-4

This project requires the use of the machine configured as win2kdc02 and the second machine running Windows 2000 professional and installed as win2kpro01.

To create a scope of IP addresses and add a client reservation:

1. Click **Start**, **Programs**, **Administrative Tools**, **DHCP on win2kdc02**.
2. Right-click your **servername** (win2kdc02), and select **New Scope**.
3. Click **Next** in the New Scope Wizard dialog box.
4. Type **Partner's Scope** in the Name field, leave the Description field blank, and click **Next** to continue.

5. In the Start IP address field, type **192.168.12.100** (or the number assigned by your instructor), and then in the End IP address field, type the same number you placed in the Start IP address field. You are creating a scope of one.
6. In the Subnet Mask field, type **255.255.255.0**.
7. Click **Next** to continue.
8. Click **Nex**t to skip the Add Exclusions part of the wizard.
9. Click **Next** to accept the default lease duration of 8 days.
10. Select the **No, I will configure these options later** radio button, and click **Next** to continue.
11. Click **Finish** to complete the New Scope Wizard.
12. On the client computer (win2kpro01), issue the ipconfig /all command at the command prompt. Note the physical address here ________________. (It should be a 12-digit hexadecimal address.)
13. Click **+** to expand the scope.
14. Right-click **Reservations** and select **New Reservation**.
15. Enter **Partner's Computer** in the Reservation name: field.
16. Type the address from Step 5 in the IP address field.
17. Type the physical address from Step 12 (minus the hyphens) in the MAC address: field.
18. Leave the Description blank and leave Supported types set to **Both**.
19. Click **Add** to add the reservation, then click **Close** to close the New Reservation dialog box.

Note

To create a superscope, select **New Superscope** in Step 2 and follow the New Superscope Wizard directions. To create a multicast scope, select **New Multicast Scope** and follow the New Multicast Scope Wizard directions.

Hands-on Project

Project 3-5

To test the scope and reservation:

1. On the DHCP server, right-click your configured scope and select **Activate**.
2. On the DHCP client machine, win2kpro01, right-click **My Network Places** and select **Properties**.
3. Right-click **Local Area Connection**, and select **Properties**.
4. Double-click **Internet Protocol (TCP/IP)** and verify on the General tab that the client is configured to Obtain an IP address automatically. (If the client has a static address, select the **Obtain an IP address automatically** radio button, and then click **OK**.)
5. Click **OK** to close the Local Area Connections Dialog Box.

6. Click **Start**, **Programs**, **Accessories**, **Command Prompt**.
7. After the command prompt, type the **ipconfig /release** command.

   This releases any previous dynamic IP addresses that may be on the client.
8. After the command prompt, type the **ipconfig /renew** command to obtain a new IP address lease.
9. The client should receive the IP address you reserved in Step 16 of Hands-on Project 3-4.
10. After the command prompt, type **ipconfig /all |more** to verify that the client did indeed receive the reserved IP address.

Project 3-6

To configure DHCP for DNS integration and allow the DHCP Server to register with DNS those clients that do not support dynamic DNS updates:

1. Click **Start**, **Programs**, **Administrative Tools**, **DHCP**.
2. Right-click your **servername** and select **Properties**.
3. Click on the **DNS tab** in the Properties Dialog box.
4. Click to select **Enable updates for DNS clients that do not support dynamic update**. Click **OK**.

   You configured your DHCP server to register clients such as Windows 95, Windows 98, and Windows NT that do not support dynamic DNS updates.

Note

Hands-on Project 3-6 sets the DNS properties for all scopes on the server because you set the property at the server level. You can also set the DNS properties on a per scope basis.

Project 3-7

To view statistics available in the DHCP snap-in:

1. Click **Start**, **Programs**, **Administrative Tools**, **DHCP**.
2. Click your **servername** to select the DHCP server.
3. Click **Action** and then select **Display Statistics**.
4. Click **Refresh** to update the statistics. Click **Close** to return to the DHCP snap-in.

Project 3-8

To stop the DHCP service, compact the DHCP server database, and restart the service:

1. Click **Start**, **Programs**, **Accessories**, **Command Prompt**.
2. Type **net stop dhcpserver** after the command prompt.

   This command stops the DHCP server service.

3. Type **cd systemroot drive letter\winnt\system32\dhcp**, and press **Enter**.
4. After the command prompt, type **jetpack dhcp.mdb temp.mdb** to compact the DHCP database. A message similar to the following appears:

   ```
   Compacted database dhcp.mdb in 1.432 seconds.
   moving temp.mdb => dhcp.mdb
   jetpack completed successfully.
   ```

5. Type **net start dhcpserver** to restart the DHCP server service.
6. Type **exit** to close the Command prompt.

Project 3-9

To configure System Monitor to examine the DHCP server service:

1. Click **Start**, **Programs**, **Administrative Tools**, **Performance**.
2. Right-click in the chart area of the right pane, and select **Add Counters**.
3. In the Performance Object box, scroll up and select **DHCP Server**.
4. Add **Discovers/sec**, **Offers/sec**, **Requests/sec**, and **Acks/sec**.
5. Click **Close** to shut the Add Counters dialog box.
6. On your Windows 2000 client machine configured for DHCP in earlier projects in this chapter, issue the **ipconfig /release** and **ipconfig /renew** commands several times, and watch DHCP activity on System Monitor.

CASE PROJECTS

Case 1

Your network is configured as shown in Figure 3-22. Your boss wants you to design a DHCP implementation that uses as few servers as possible. Create two possible plans for supporting DHCP on this network.

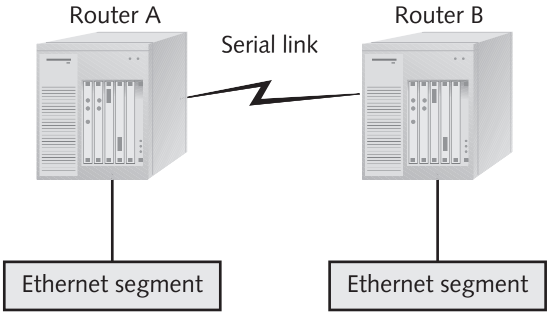


Figure 3-22 Example Network

Case 2

Hillier, Inc. has hired you to install DHCP services. For the initial meeting, prepare a short summary of new features in the Windows 2000 DHCP server service. For the summary, prepare a preliminary design for scopes and option assignments. (Determine how many scopes are needed, how many servers, what options must be specified.)

Case 3

After your meeting at Hillier, Inc., the chief information officer, Merlin, sends you an e-mail questioning the need for Active Directory in the design of DHCP services. Draft a quick e-mail to the CIO detailing the benefits Active Directory brings to a DHCP implementation.